PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-277664
(43)Date of publication of application : 22.10.1996

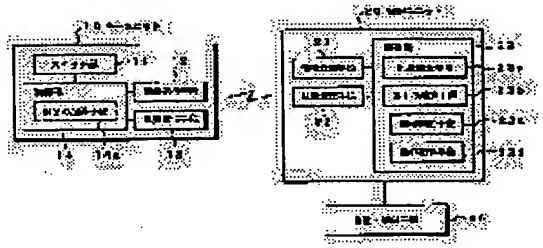
(51)Int.Cl. E05B 49/00
B60J 5/00
E05B 65/20

(21)Application number : 07-080079
(22)Date of filing : 05.04.1995

(71)Applicant : OKI ELECTRIC IND CO LTD
(72)Inventor : KISHI KAZUYA

(54) ELECTRONIC KEY SYSTEM

(57)Abstract:
PURPOSE: To provide an electronic key system having a very low possibility of being decoded by calculating coded functions based on authentication codes and random numbers at both a control unit and a key unit, and collating them.
CONSTITUTION: When the prescribed information is transmitted from a key unit 10, a control unit 20 generates a random number with a random number generating means 23a in response to it and sends it to the key unit 10. The control unit 20 also calculates the coded function with the first arithmetic means 23b based on the random number and the inherent authentication code. The key unit 10 calculates the coded function with the second arithmetic means 14a based on the received random number and the inherent authentication code and transmits it to the control unit 20. The control unit 20 collates both coded functions with a code judging means 23c, judges whether the prescribed conditions are satisfied or not, and controls a locking/unlocking means based on it for locking or unlocking.



LEGAL STATUS

[Date of request for examination] 22.02.2002
[Date of sending the examiner's decision of rejection] 06.09.2005
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's

decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平8－277664

(43)公開日　平成８年(1996)10月22日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｅ０５Ｂ　49/00			Ｅ０５Ｂ　49/00	Ｊ	
Ｂ６０Ｊ　5/00			Ｂ６０Ｊ　5/00	Ｍ	
Ｅ０５Ｂ　65/20			Ｅ０５Ｂ　65/20		

審査請求　未請求　請求項の数２　ＯＬ　（全 11 頁）

(21)出願番号　特願平7－80079

(22)出願日　平成７年(1995)４月５日

(71)出願人　000000295
沖電気工業株式会社
東京都港区虎ノ門１丁目７番12号

(72)発明者　岸　和也
東京都港区虎ノ門１丁目７番12号　沖電気工業株式会社内

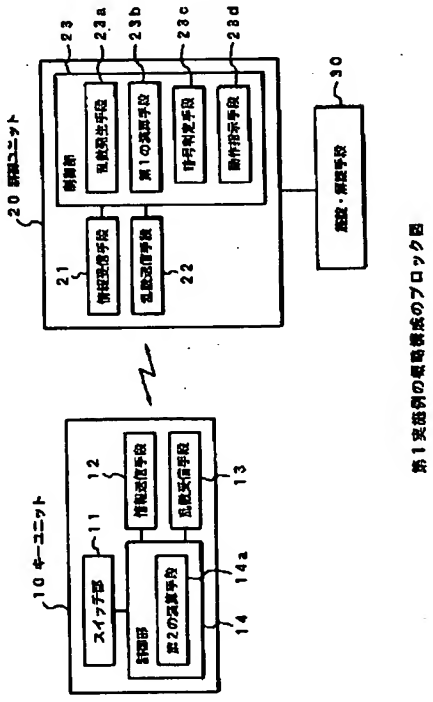
(74)代理人　弁理士　船橋　國則

(54)【発明の名称】　電子キーシステム

(57)【要約】

【目的】　本発明は、例えば赤外光や電波等を用いて施錠または解錠を行うもので、施錠または解錠を行う際に暗証コードが直接送受信されることのない電子キーシステムを提供することを目的とする。

【構成】　キーユニット１０と制御ユニット２０と施錠・解錠手段３０とから構成され、前記キーユニット１０及び前記制御ユニット２０がそれぞれ固有の暗証コードを有する電子キーシステムにおいて、キーユニット１０と制御ユニット２０との間では、乱数と、その乱数及び前記暗証コードより演算された暗号化関数とが送受信されることにより互いの認証を行って、その結果施錠・解錠手段３０で施錠または解錠が行われることを特徴とする。



第１実施例の電動錠装置のブロック図

1

【特許請求の範囲】

【請求項1】　情報を送信する情報送信手段を備えたキーユニットと、

前記情報送信手段から送信された情報を受信する情報受信手段を備えた制御ユニットと、

該制御ユニットからの指示に従い施錠または解錠を行う施錠・解錠手段とから構成され、

前記キーユニットと前記制御ユニットとはそれぞれ固有の暗証コードを有している電子キーシステムにおいて、

前記制御ユニットには、前記情報送信手段からの所定の情報を前記情報受信手段で受信すると乱数を発生する乱数発生手段と、

該乱数発生手段が発生した乱数と前記制御ユニットに固有の暗証コードとを基に暗号化関数を演算する第1の演算手段と、

前記乱数発生手段が発生した乱数を前記キーユニットに送信する乱数送信手段とが設けられ、

前記キーユニットには、前記乱数送信手段から送信された乱数を受信する乱数受信手段と、

該乱数受信手段で受信した乱数と前記キーユニットに固有の暗証コードとを基に暗号化関数を演算する第2の演算手段とが設けられ、

さらに、前記制御ユニットには、前記第2の演算手段で演算された暗号化関数が前記情報送信手段から前記情報受信手段へ送信されると、送信された暗号化関数と前記第1の演算手段で演算された暗号化関数とが予め設定された所定の条件を満足するか否かを判定する暗号判定手段と、

該暗号判定手段が所定の条件を満足すると判定した場合に、前記施錠・解錠手段に施錠または解錠を行うように指示を与える動作指示手段とが設けられたことを特徴とする電子キーシステム。

【請求項2】　前記キーユニットには、該キーユニットに固有の暗証コードを記憶する第1の記憶手段が設けられ、

前記制御ユニットには、該制御ユニットに固有の暗証コードを記憶する第2の記憶手段が設けられ、

前記キーユニットと前記制御ユニットとの少なくとも一方に新たな暗証コードを送信する書き換え指示手段と、

前記暗号判定手段により前記第1の演算手段で演算された暗号化関数と前記第2の演算手段で演算された暗号化関数とが所定の条件を満足すると判定された後に、前記書き換え指示手段から前記新たな暗証コードが送信されると、前記第1の記憶手段に記憶されている暗証コードと前記第2の記憶手段に記憶されている暗証コードとの両方を前記新たな暗証コードに書き換える暗証コード書き換え手段とを備えてなることを特徴とする請求項1記載の電子キーシステム。

【発明の詳細な説明】

【0001】

2

【産業上の利用分野】本発明は、例えば赤外光や電波等を用いて施錠または解錠を行う電子キーシステムに関するものである。

【0002】

【従来の技術】従来、電子キーシステムとしては、例えば自動車のドアに用いられているものが知られている。この電子キーシステムは、赤外光や電波等を介することによって、使用者が非接触で自動車のドアの施錠または解錠を行えるようにしたものであり、図5に示すように、使用者が携帯するキーユニット50と、自動車のドアに設けられている制御ユニット60と、ドアの施錠または解錠を行うソレノイド70とから構成されているものである。

【0003】キーユニット50は、このキーユニット50に固有の暗証コードを、例えば予め回路上のパターンに刻み込まれたことによって有しているものであり、さらに、使用者が操作するためのスイッチ部51と、赤外光や電波等を介して前記暗証コードを送信する送信部52とを備えてなるものである。制御ユニット60は、キーユニット50と同様にこの制御ユニット60に固有な暗証コードを有しているものであり、さらに、受信部61と、判定部62と、動作指示部63とを備えてなるものである。受信部61は、キーユニット50の送信部52からの暗証コードを受信するものである。判定部62は、受信部61で受信した暗証コードと制御ユニット60が有している暗証コードとが一致するか否かを判定するものである。動作指示部63は、判定部62による判定結果に従い、ソレノイド70に対して動作指示を行うものである。

【0004】このような電子キーシステムでは、使用者がキーユニット50のスイッチ部51を操作すると、送信部52がこのキーユニット50の有している暗証コードを赤外光や電波等を介して制御ユニット60へ送信する。キーユニット50から暗証コードが送信されると、制御ユニット60では、受信部61でその暗証コードを受信し、判定部62で受信した暗証コードとこの制御ユニット60の有している暗証コードとが一致するか否かを判定する。そして、判定部62によりそれぞれの暗証コードが一致すると判定されると、動作指示部63では、ソレノイド70に対して動作指示を与える。従って、キーユニット50に固有の暗証コードと制御ユニット60に固有の暗証コードとが一致すれば、ソレノイド70の動作によってドアの施錠または解錠が行われる。

【0005】

【発明が解決しようとする課題】しかしながら、上述した電子キーシステムでは、キーユニット50と制御ユニット60との間で暗証コードが直接送受信されるようになっているため、第三者にその暗証コードが解読されてしまい、キーユニットが偽造される恐れがある。

【0006】また、上述した電子キーシステムは、暗証

3

コードが同一であるキーユニット５０及び制御ユニット６０を一対とすると、他のキーユニットによる施錠または解錠を防ぐために、各対毎に異なる暗証コードを有していなければならない。但し、キーユニット５０及び制御ユニット６０には、予め暗証コードが回路上のパターン等に刻み込まれているので、例えば製造過程や保守交換時等においてはキーユニット５０及び制御ユニット６０を各対毎、即ち暗証コード毎に管理しなければならず、その管理が煩雑なものとなってしまい、製造過程や保守交換時等における作業効率の低下の一因となってしまう。そのために、例えばキーユニット５０及び制御ユニット６０の有している暗証コードを書き換え可能にすることが考えられるが、この場合に第三者であっても暗証コードの書き換えが可能であると、電子キーシステムとしての機能を果たさなくなってしまう。

【０００７】そこで、本発明は、施錠または解錠を行う際に暗証コードが直接送受信されることのない電子キーシステムを提供することを目的とする。さらに、本発明は、第三者に暗証コードが書き換えられることなく、所望する暗証コードに書き換えることが可能な電子キーシステムを提供することを目的とする。

【０００８】

【課題を解決するための手段】本発明は、上記目的を達成するために案出された電子キーシステムで、情報を送信する情報送信手段を備えたキーユニットと、前記送信手段から送信された情報を受信する情報受信手段を備えた制御ユニットと、この制御ユニットからの指示に従い施錠または解錠を行う施錠・解錠手段とから構成され、前記キーユニットと前記制御ユニットとはそれぞれ固有の暗証コードを有しているものであり、その上、前記制御ユニットには、前記情報送信手段からの所定の情報を前記情報受信手段で受信すると乱数を発生する乱数発生手段と、この乱数発生手段が発生した乱数と前記制御ユニットに固有の暗証コードとを基に暗号化関数を演算する第１の演算手段と、前記乱数発生手段が発生した乱数を前記キーユニットに送信する乱数送信手段とが設けられ、一方、前記キーユニットには、前記乱数送信手段から送信された乱数を受信する乱数受信手段と、この乱数受信手段で受信した乱数と前記キーユニットに固有の暗証コードとを基に暗号化関数を演算する第２の演算手段とが設けられ、さらに、前記制御ユニットには、前記第２の演算手段で演算された暗号化関数が前記情報送信手段から前記情報受信手段へ送信されると、送信された暗号化関数と前記第１の演算手段で演算された暗号化関数とが予め設定された所定の条件を満足するか否かを判定する暗号判定手段と、この暗号判定手段が所定の条件を満足すると判定した場合に、前記施錠・解錠手段に施錠または解錠を行うように指示を与える動作指示手段とが設けられたことを特徴とする。

【０００９】また、前記キーユニットには、このキーユニットに固有の暗証コードを記憶する第１の記憶手段が設けられ、前記制御ユニットには、この制御ユニットに固有の暗証コードを記憶する第２の記憶手段が設けられ、さらに、前記キーユニットと前記制御ユニットとの少なくとも一方に新たな暗証コードを送信する書き換え指示手段と、前記暗号判定手段により前記第１の演算手段で演算された暗号化関数と前記第２の演算手段で演算された暗号化関数とが所定の条件を満足すると判定された後に、前記書き換え指示手段から前記新たな暗証コードが送信されると、前記第１の記憶手段に記憶されている暗証コードと前記第２の記憶手段に記憶されている暗証コードとの両方を前記新たな暗証コードに書き換える暗証コード書き換え手段とを備えてなるものであってもよい。

4

【００１０】

【作用】上記構成の電子キーシステムによれば、以下のような作用を奏する。先ず、キーユニットの情報送信手段から所定の情報が送信されると、制御ユニットでは、情報受信手段でその情報を受信し、その情報に対応して乱数発生手段で乱数を発生して、その乱数を乱数送信手段でキーユニットへ送信する。これと同時に、制御ユニットでは、乱数発生手段で発生した乱数とこの制御ユニットに固有の暗証コードとを基に、第１の演算手段で暗号化関数を演算する。一方、キーユニットでは、制御ユニットの乱数送信手段から乱数が送信されると、乱数受信手段でその乱数を受信し、その乱数とこのキーユニットに固有の暗証コードとを基に第２の演算手段で暗号化関数を演算し、その暗号化関数を情報送信手段で制御ユニットへ送信する。そして、制御ユニットでは、キーユニットの情報送信手段からの暗号化関数を情報受信手段で受信すると、暗号判定手段によって受信した暗号化関数と第１の演算手段で演算した暗号化関数とが所定の条件を満足するか否かを判定する。このとき、第１の演算手段は、乱数発生手段が発生した乱数と制御ユニットに固有の暗証コードとを基に暗号化関数を演算し、また、第２の演算手段は、乱数発生手段が発生した乱数とキーユニットに固有の暗証コードとを基に暗号化関数を演算している。よって、例えば、制御ユニットに固有の暗証コードとキーユニットに固有の暗証コードとがそれぞれ同一であり、かつ、第１の演算手段と第２の演算手段とが同一の演算を行えば、前記第１の演算手段による暗号化関数と前記第２の演算手段による暗号化関数とは共に一致する。そして、暗号判定手段により判定される所定の条件が、例えば第１の演算手段による暗号化関数と第２の演算手段による暗号化関数とが共に一致することであれば、前記暗号判定手段では、それぞれの暗号化関数が所定の条件を満足すると判定する。暗号判定手段によりそれぞれの暗号化関数が所定の条件を満足すると判定された場合には、動作指示手段が施錠・解錠手段に施錠または解錠を行うように指示を与え、前記施錠・解錠手

5

段において施錠または解錠が行われる。

【００１１】また、キーユニットに第１の記憶手段を設け、制御ユニットに第２の記憶手段を設け、さらに書き換え指示手段と暗証コード書き換え手段とを備えれば、以下のような作用を奏する。第１の記憶手段では、キーユニットに固有の暗証コードを記憶している。また、第２の記憶手段では、制御ユニットに固有の暗証コードを記憶している。ここで、暗号判定手段により第１の演算手段で演算された暗号化関数と第２の演算手段で演算された暗号化関数とが所定の条件を満足すると判定された後に、書き換え指示手段から新たな暗証コードが送信されると、暗証コード書き換え手段では、第１の記憶手段に記憶されている暗証コードと第２の記憶手段に記憶されている暗証コードとの両方を前記新たな暗証コードに書き換える。従って、第１の記憶手段及び第２の記憶手段には、新たな暗証コードがそれぞれに固有な暗証コードとして記憶される。

【００１２】

【実施例】以下、図面に基づき本発明に係わる電子キーシステムについて説明する。但し、ここでは、本発明を自動車のドアの施錠または解錠を行う電子キーシステムに適用した場合について説明する。

【００１３】〔第１実施例〕本実施例の電子キーシステムは、請求項１記載の発明に係わる電子キーシステムであり、図１に示すように、キーユニット１０と、制御ユニット２０と、施錠・解錠手段３０とを備えて構成されるものである。

【００１４】キーユニット１０は、使用者が携帯できるようになっているもので、スイッチ部１１と、情報送信手段１２と、乱数受信手段１３と、制御部１４とを備えてなるものである。スイッチ部１１は、押しボタンスイッチ等からなるもので、使用者が自動車のドアの施錠または解錠を行うためにＯＮするものである。情報送信手段１２は、赤外光や電波等を発信することにより、後述する情報を制御部１４からの指示に従い、制御ユニット２０へ送信するものである。乱数受信手段１３は、後述する制御ユニット２０の乱数送信手段２２から乱数Ｒの格納されている情報が送信されると、その情報を受信するものである。

【００１５】制御部１４は、ＣＰＵ（central processing unit）等からなるもので、例えばこの制御部１４の回路上のパターンに予めこのキーユニット１０に固有な暗証コードK-codeを保持しているとともに、第２の演算手段１４ａを備えたものである。第２の演算手段１４ａは、乱数受信手段１３で受信した情報から乱数Ｒを取り出して、この乱数ＲとキーユニットＩ０に固有な暗証コードK-codeとを基に、暗号化関数f(R,K-code)を演算するものである。また、この制御部１４では、スイッチ部１１がＯＮされると“ASK(R)”というコマンドを、さらに第２の演算手段１４ａが暗号化関数f(R,K-code)を演算すると、その暗号化関数f(R,K-code)を格納した“SEND(f(R,K-code))”というコマンドを、それぞれ制御ユニット２０へ送信するように情報送信手段１２に対して指示を与えるようになっている。

6

【００１６】制御ユニット２０は、自動車のドアに設けられているもので、情報受信手段２１と、乱数送信手段２２と、制御部２３とを備えてなるものである。情報受信手段２１は、キーユニット１０の情報送信手段１２からの情報、即ち“ASK(R)”というコマンドと“SEND(f(R,K-code))”というコマンドとを受信するものである。乱数送信手段２２は、制御部２３の指示に従い、後述する乱数発生手段２３ａが発生した乱数Ｒを“RETURN(R)”というコマンドに格納し、赤外光や電波等を用いてキーユニット１０の乱数受信手段１３へ送信するものである。

【００１７】制御部２３は、ＣＰＵ等からなるもので、キーユニット１０の制御部１４と同様にこの制御ユニット２０に固有な暗証コードK-codeを保持しているとともに、乱数発生手段２３ａと、第１の演算手段２３ｂと、暗号判定手段２３ｃと、動作指示手段２３ｄとを備えてなるものである。但し、この制御部２３では、キーユニット１０の制御部１４と同一の暗証コードK-codeを保持しているものとする。乱数発生手段２３ａは、情報受信手段２１が情報送信手段１２からの“ASK(R)”というコマンドを受信すると、乱数Ｒを発生するものである。第１の演算手段２３ｂは、乱数発生手段２３ａが乱数Ｒを発生すると、その乱数Ｒと制御ユニット２０に固有な暗証コードK-codeとを基に、暗号化関数f(R,K-code)を演算するものである。但し、この第１の演算手段２３ｂでは、第２の演算手段１４ａと同じ暗号化関数f(R,K-code)を演算するようになっている。

【００１８】暗号判定手段２３ｃは、情報受信手段２１が情報送信手段１２からの“SEND(f(R,K-code))”というコマンドを受信すると、そのコマンドより第２の演算手段１４ａで演算された暗号化関数f(R,K-code)を取り出して、この暗号化関数f(R,K-code)と第１の演算手段２３ｂで演算された暗号化関数f(R,K-code)とが予め設定されている所定の条件を満足するか否か、即ち、第１の演算手段２３ｂによる暗号化関数f(R,K-code)と第２の演算手段１４ａによる暗号化関数f(R,K-code)とが一致するか否かを判定するものである。動作指示手段２３ｄは、暗号判定手段２３ｃにおいて第１の演算手段２３ｂによる暗号化関数f(R,K-code)と、第２の演算手段１４ａによる暗号化関数f(R,K-code)とが一致すると判定されると、施錠・解錠手段３０に対してドアの施錠または解錠を行うように指示を与えるものである。

【００１９】施錠・解錠手段３０は、ソレノイド等からなり、制御ユニット２０と同様に自動車のドアに設けられ、かつその制御ユニット２０と電気的に接続されているものである。また、制御ユニット２０では、動作指示

7

手段２３ｄからの指示に従って、例えば自動車のドアが施錠されていれば解錠を、また自動車のドアが解錠されていれば施錠を行うようになっている。

【００２０】次に、以上のように構成された電子キーシステムにおいて、自動車のドアの施錠または解錠を行う動作例について、図２のフローチャートに従い説明する。キーユニット１０では、赤外光や電波等が制御ユニット２０に届く範囲内において使用者によりスイッチ部１１がＯＮされると（ステップ１０１、以下ステップをＳと略す）、情報送信手段１２が制御部１４の指示に従い“ASK(R)”というコマンドを制御ユニット２０へ送信する（Ｓ１０２）。情報送信手段１２から“ASK(R)”というコマンドが送信されると、制御ユニット２０では、情報受信手段２１でそのコマンドを受信し（Ｓ１０３）、さらに乱数発生手段２３ａで乱数Ｒを発生させる（Ｓ１０４）。

【００２１】乱数発生手段２３ａが乱数Ｒを発生させると、制御ユニット２０では、乱数送信手段２２がその乱数Ｒを格納した“RETURN(R)”というコマンドをキーユニット１０へ送信し、かつ、第１の演算手段２４が前記乱数Ｒとこの制御ユニット２０に固有な暗証コードK-codeとを基に、暗号化関数f(R,K-code)の演算を行う（Ｓ１０５）。一方、キーユニット１０では、乱数送信手段２２から送信された“RETURN(R)”というコマンドを乱数受信手段１３で受信すると（Ｓ１０６）、第２の演算手段１４ａが受信したコマンドから乱数Ｒを取り出し、その乱数Ｒとキーユニット１０に固有な暗証コードK-codeとを基に、暗号化関数f(R,K-code)の演算を行う（Ｓ１０７）。

【００２２】第２の演算手段１４ａで暗号化関数f(R,K-code)が演算されると、情報送信手段１２では、この暗号化関数f(R,K-code)を格納した“SEND(f(R,K-code))”というコマンドを制御ユニット２０へ送信する（Ｓ１０８）。情報送信手段１２から“SEND(f(R,K-code))”というコマンドが送信されると、制御ユニット２０では、そのコマンドを情報受信手段２１で受信する（Ｓ１０９）。そして、暗号判定手段２３ｃでは、“SEND(f(R,K-code))”というコマンドから第２の演算手段１４ａで演算された暗号化関数f(R,K-code)を取り出して、その暗号化関数f(R,K-code)と第１の演算手段２３ｂで演算された暗号化関数f(R,K-code)とが一致するか否かを判定する（Ｓ１１０）。

【００２３】このとき、第１の演算手段２３ｂでは、乱数発生手段２３ａが発生した乱数Ｒと制御ユニット２０に固有な暗証コードK-codeとを基に、暗号化関数f(R,K-code)の演算を行っている。また、第２の演算手段１４ａでは、乱数受信手段１３で受信した乱数Ｒ、即ち乱数発生手段２３ａが発生した乱数Ｒとキーユニット１０に固有な暗証コードK-codeとを基に、暗号化関数f(R,K-code)の演算を行っている。従って、制御ユニット２０に

8

固有な暗証コードK-codeと、キーユニット１０に固有な暗証コードK-codeとがそれぞれ同一であれば、第１の演算手段２３ｂによる暗号化関数f(R,K-code)と、第２の演算手段１４ａによる暗号化関数f(R,K-code)とは共に一致する。

【００２４】暗号判定手段２３ｃで第１の演算手段２３ｂによる暗号化関数f(R,K-code)と、第２の演算手段１４ａによる暗号化関数f(R,K-code)とが一致すると判定された場合、即ちキーユニット１０と制御ユニット２０との暗証コードK-codeが互いに同一である場合には、動作指示手段２３ｄからの指示に従い、施錠・解錠手段３０では、自動車のドアの施錠または解錠を行う（Ｓ１１１）。また、暗号判定手段２３ｃで第１の演算手段２３ｂによる暗号化関数f(R,K-code)と、第２の演算手段１４ａによる暗号化関数f(R,K-code)とが一致しない判定された場合には、キーユニット１０と制御ユニット２０との暗証コードK-codeが互いに異なるので、動作指示手段２３ｄでは、施錠または解錠を行う指示を与えない。よって、施錠・解錠手段３０では、自動車のドアの施錠または解錠を行わない。

【００２５】このように本実施例の電子キーシステムでは、キーユニット１０と制御ユニット２０との間において、乱数発生手段２３ａが発生した乱数Ｒと、第２の演算手段１４ａが演算した暗号化関数f(R,K-code)とを送受信するようになっている。従って、キーユニット１０と制御ユニット２０との間で暗証コードK-codeが直接送受信されることがなく、さらに乱数Ｒ及び暗号化関数f(R,K-code)は送受信を行う度に異なった値となるので、第三者に暗証コードK-codeが解読されドアが解錠されてしまう可能性を極めて低くすることができる。

【００２６】〔第２実施例〕次に、請求項２記載の発明に係わる電子キーシステムについて説明する。但し、上述した第１実施例と同一の構成要素については、同一の符号を与えてその説明を省略する。本実施例の電子キーシステムは、図３に示すように、キーユニット１０ａと、制御ユニット２０ａと、施錠・解錠手段３０と、書き換え指示手段４０とを備えて構成されるものである。

【００２７】キーユニット１０ａは、上述した第１実施例に加えて、第１の記憶手段１５が設けられたものである。第１の記憶手段１５は、例えばＥＥＰＲＯＭ（Electrically Erasable Progr-ammable Read-Only Memory）のような電気的に書き込み及び読み出しが可能な不揮発性メモリからなるもので、キーユニット１０ａに固有な暗証コードを記憶するためのものである。従って、このキーユニット１０ａでは、第１実施例と異なり、暗証コードK-codeが制御部１４に保持されているのではなく、第１の記憶手段１５に記憶されるようになっている。

【００２８】制御ユニット２０ａは、上述した第１実施例に加えて、第２の記憶手段２４が設けられ、かつ、制御部２３が暗証コード書き換え手段２３ｅを備えている

ものである。第２の記憶手段２４は、第１の記憶手段１５と同様に不揮発性メモリからなるもので、制御ユニット２０ａに固有な暗証コードを記憶するためのものである。従って、この制御ユニット２０ａでは、キーユニット１０ａと同様に、暗証コードK-codeが制御部２３に保持されているのではなく、第２の記憶手段２４に記憶されるようになっている。

【００２９】暗証コード書き換え手段２３ｅは、暗号判定手段２３ｃにおいて第１の演算手段で２３ｂによる暗号化関数f(R,K-code) と第２の演算手段１４ａによる暗号化関数f(R,K-code) とが互いに一致すると判定された後に、後述する書き換え指示手段４０から新たな暗証コードK-code' が送信されると、第１の記憶手段１５に記憶されている暗証コードK-codeと第２の記憶手段２４に記憶されている暗証コードK-codeとの両方を新たな暗証コードK-code' に書き換えるものである。即ち、暗証コード書き換え手段２３ｅでは、暗号判定手段２３ｃでキーユニット１０ａと制御ユニット２０ａとの暗証コードK-codeが互いに一致すると判定された後、予めこの暗証コード書き換え手段２３ｅに設定されている所定時間内に、後述する書き換え指示手段４０からの“REWRITE(K-code')”というコマンドを情報受信手段２１で受信すると、そのコマンドから新たな暗証コードK-code' を取り出して、第２の記憶手段２４に記憶されている暗証コードK-codeを、新たな暗証コードK-code' に書き換えるようになっている。さらに、暗証コード書き換え手段２３ｅでは、取り出した新たな暗証コードK-code' を“RETURN(K-code')”というコマンドに格納して、乱数送信手段２２から乱数受信手段１３へ送信し、キーユニット１０ａに対して第１の記憶手段１５に記憶されている暗証コードK-codeを、新たな暗証コードK-code' に書き換えるように指示を与えるようになっている。尚、乱数送信手段２２と乱数受信手段１３との間では、乱数発生手段２３ａが発生した乱数Ｒに加え、“RETURN(K-code')”というコマンドが送受信されるようになっている。

【００３０】書き換え指示手段４０は、制御ユニット２０ａに赤外光や電波等が届く範囲内において用いられるもので、スイッチ部４１と、情報送信手段４２と、暗証コード格納部４３と、制御部４４とを備えてなるものである。スイッチ部４１は、キーユニット１０ａのスイッチ部１１と同様に構成されたものであり、また情報送信手段４２は、キーユニット１０ａの情報送信手段１２と同様に構成されたものである。暗証コード格納部４３は、書き換えようとする新たな暗証コードK-code' を予め保持しているものであり、例えばキーユニット１０ａの第１の記憶手段１５と同様に不揮発性メモリからなるものである。但し、暗証コード格納部４３は、例えばキーボード等の外部装置に接続されて、この外部装置で設定された新たな暗証コードK-code' を受け取るように構成されたものであってもよい。

【００３１】制御部４４は、キーユニット１０ａの制御部１４と同様にＣＰＵ等からなるものである。但し、この制御部４４では、スイッチ部４１が押圧されると、暗証コード格納部４３に保持されている新たな暗証コードK-code' を、“REWRITE(K-code')”というコマンドに格納し、そのコマンドを制御ユニット２０ａへ送信するように情報送信手段４２に対して指示を与えるようになっている。つまり、書き換え指示手段４０は、上述した機能を有するものであれば、例えばキーユニット１０ａと同様に構成されたものであってもよい。また、書き換え指示手段４０は、例えばキーユニット１０ａに上述した機能を追加したもの、即ちキーユニット１０ａと一体に構成されたものであってもよい。

【００３２】次に、以上のように構成された電子キーシステムにおいて、暗証コードを書き換える動作例について、図４のフローチャートに従い説明する。但し、使用者がキーユニット１０ａのスイッチ部１１をＯＮするステップから、暗号判定手段２３ｃにおいてキーユニット１０ａと制御ユニット２０ａとの暗証コードK-codeが互いに同一であるか否かを判定するステップまでは（図４におけるＳ２０１～Ｓ２１０）、第１実施例と同様であるのでその説明を省略する。また、本実施例における施錠または解錠を行う動作例は、第１実施例と同様であるのでその説明を省略する。尚、キーユニット１０ａの第１の記憶手段１５と制御ユニット２０ａの第２の記憶手段２４には、予め同一の暗証コードK-codeが記憶されているものとする。

【００３３】暗号判定手段２３ｃで暗証コードK-codeが互いに同一であると判定されると、続いて使用者は、書き換え指示手段４０のスイッチ部４１をＯＮする（Ｓ２１１）。但し、暗号判定手段２３ｃで暗証コードK-codeが互いに同一でないと判定されると、暗証コードK-codeが同一でないキーユニット１０ａ及び制御ユニット２０ａは、暗証コードK-codeを書き換える条件を満たしていないので、使用者がスイッチ部４１をＯＮしても書き換え動作は行われない。スイッチ部４１がＯＮされると、書き換え指示手段４０の情報送信手段４２は、制御部４４の指示に従って、新たな暗証コードK-code' を格納した“REWRITE(K-code')”というコマンドを制御ユニット２０ａへ送信する（Ｓ２１２）。

【００３４】情報送信手段４２から“REWRITE(K-code')”というコマンドが送信されると、制御ユニット２０ａでは、情報受信手段２１でそのコマンドを受信する（Ｓ２１３）。そして、暗証コード書き換え手段２３ｅでは、暗号判定手段２３ｃで暗証コードK-codeが互いに同一であると判定されてから、情報受信手段２１で“REWRITE(K-code')”というコマンドを受信するまでの時間が、この暗証コード書き換え手段２３ｅに設定されている所定時間内であるか否かを判定する（Ｓ２１４）。即ち、暗証コード書き換え手段２３ｅでは、使用者がキー

11

ユニット１０ａのスイッチ部１１をＯＮしてから、所定時間内に書き換え指示手段４０のスイッチ部４１をＯＮしたか否かを判定する。

【００３５】使用者が所定時間内にスイッチ部４１をＯＮしなかった場合には、暗証コード書き換え手段２３ｅにより暗証コードK-codeを書き換える条件が満たされていないと判断され、書き替え動作は行われない。また、使用者が所定時間内にスイッチ部４１をＯＮした場合には、暗証コード書き換え手段２３ｅでは、情報受信手段２１で受信した“REWRITE(K-code')”というコマンドから新たな暗証コードK-code'を取り出して、その暗証コードK-code'を第２の記憶手段２４に書き込む（Ｓ２１５）。これと同時に、暗証コード書き換え手段２３ｅでは、取り出した暗証コードK-code'を“RETURN(K-code')”というコマンドに格納して乱数送信手段２２へ送出する。そして、乱数送信手段２２では、“RETURN(K-code')”というコマンドをキーユニット１０ａへ送信する（Ｓ２１６）。

【００３６】乱数送信手段２２から“RETURN(K-code')”というコマンドが送信されると、キーユニット１０ａでは、乱数受信手段１３でそのコマンドを受信する（Ｓ２１７）。乱数受信手段１３が“RETURN(K-code')”というコマンドを受信すると、制御部１４では、そのコマンドから新たな暗証コードK-code'を取り出して、その暗証コードK-code'を第１の記憶手段１５に書き込む（Ｓ２１８）。従って、第１の記憶手段１５及び第２の記憶手段２４には、共に新たな暗証コードK-code'が、それぞれに固有な暗証コードとして記憶される。

【００３７】このように本実施例の電子キーシステムでは、キーユニット１０ａに固有な暗証コードK-codeが第１の記憶手段１５に記憶され、また制御ユニット２０ａに固有な暗証コードK-codeが第２の記憶手段２４に記憶され、これらの暗証コードK-codeが書き換え指示手段４０からの指示に従い、暗証コード書き換え手段２３ｅによって書き換えられるようになっている。従って、例えば製造過程において、予め全てのキーユニット１０ａ及び制御ユニット２０ａに同一の暗証コードK-codeを記憶させ、出荷時に対となるキーユニット１０ａ及び制御ユニット２０ａに新たな暗証コードK-code'を個別に記憶させるといったことが可能となるので、キーユニット１０ａ及び制御ユニット２０ａを各対毎に管理する必要がなくなり、結果として管理の煩雑さを低減することができる。

【００３８】また、本実施例の電子キーシステムでは、自動車のドアに搭載した後でも暗証コードK-codeの書き換えが行えるので、例えばキーユニット１０ａと制御ユニット２０ａとのいずれか一方に不具合が発生しても、キーユニット１０ａと制御ユニット２０ａとを一対として交換することなく、いずれか一方の交換及び暗証コードK-codeの書き換えにより対応することができ、保守交換時における柔軟な対応が可能となる。つまり、本実施例の電子キーシステムでは、暗証コードK-codeの管理の煩雑さを低減することにより、製造過程や保守交換時等における作業効率の向上を図ることができる。

12

【００３９】さらに、本実施例の電子キーシステムでは、暗号判定手段２３ｃにおいてキーユニット１０ａと制御ユニット２０ａとの暗証コードK-codeが互いに同一であると判定された後に、書き換え指示手段４０からの指示があれば、暗証コード書き換え手段２３ｅが新たな暗証コードK-code'への書き換えを行うようになっている。従って、キーユニット１０ａ及び制御ユニット２０ａが互いに同一である暗証コードK-codeを既に有している場合のみ、新たな暗証コードK-code'への書き換えが行われるので、第三者に暗証コードK-codeが書き換えられてしまう可能性が極めて低くなる。

【００４０】尚、上述した第１実施例及び第２実施例では、本発明を自動車のドアに適用した場合について説明したが、本発明はこれに限定されるものではなく、例えば家屋のドアやロッカーの扉等にも適用可能である。また、上述した第１実施例及び第２実施例では、第１の演算手段２３ｂ及び第２の演算手段１４ａが同一の暗号化関数f(R,K-code)を演算し、かつ暗号判定手段２３ｃでそれぞれの演算結果が一致するか否かを判定する場合について説明したが、例えば第１の演算手段２３ｂと第２の演算手段１４ａとで異なる暗号化関数f(R,K-code)を演算し、かつそれぞれの暗号化関数f(R,K-code)が所定の条件として予め暗号判定手段２３ｃに設定され、この暗号判定手段２３ｃによってそれぞれの演算結果が予め設定されている所定の条件を満足するか否か判定される場合であってもよい。さらに、上述した第２実施例では、暗証コード書き換え手段２３ｅを制御ユニット２０ａの制御部２３に設けた場合について説明したが、例えば暗証コード書き換え手段２３ｅをキーユニット１０ａの制御部１４に設けてもよい。

【００４１】

【発明の効果】以上に説明したように、本発明の電子キーシステムは、キーユニットと制御ユニットとの間において、乱数発生手段が発生した乱数と第２の演算手段が演算した暗号化関数とを送受信するようになっている。従って、キーユニットと制御ユニットとの間で暗証コードが直接送受信されることがなく、さらに乱数及び暗号化関数は送受信を行う度に異なった値となるので、第三者に暗証コードが解読される可能性が極めて低くなり、暗証コードの解読による施錠または解錠を防ぐことができるという効果を奏する。

【００４２】また、キーユニットに第１の記憶手段を、制御ユニットに第２の記憶手段をそれぞれ設け、さらに書き換え指示手段と暗証コード書き換え手段とを備えれば、暗号判定手段が所定の条件を満足すると判定し、か

13

つ書き換え指示手段からの指示があった場合に、暗証コード書き換え手段によって暗証コードが書き換えられるようになっている。従って、キーユニット及び制御ユニットの暗証コードの書き換えが可能となるので、キーユニット及び制御ユニットを各対毎に管理する必要がなくなり、結果として管理の煩雑さを低減することが可能となり、例えば製造過程や保守交換時等における作業効率の向上を図ることができる。但し、キーユニット及び制御ユニットでは、暗号判定手段が所定の条件を満足すると判定した場合にのみ新たな暗証コードへの書き換えが行われるので、第三者に書き換えられてしまう可能性を極めて低くした上での暗証コードの書き換えを実現することができる。

【図面の簡単な説明】

【図1】本発明に係わる電子キーシステムの第1実施例の概略構成を示すブロック図である。

【図2】図1の電子キーシステムにおける施錠または解錠の動作例を示すフローチャートである。

【図3】本発明に係わる電子キーシステムの第2実施例の概略構成を示すブロック図である。

【図4】図3の電子キーシステムにおける暗証コードの

14

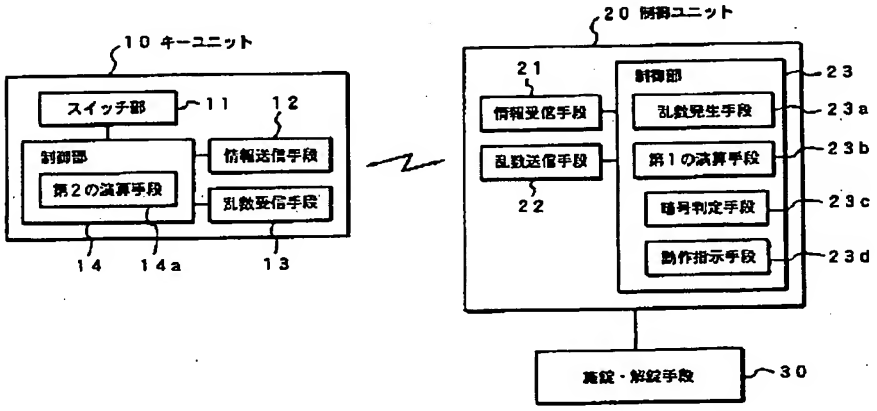
書き換えの動作例を示すフローチャートである。

【図5】従来例の電子キーシステムの概略構成を示すブロック図である。

【符号の説明】

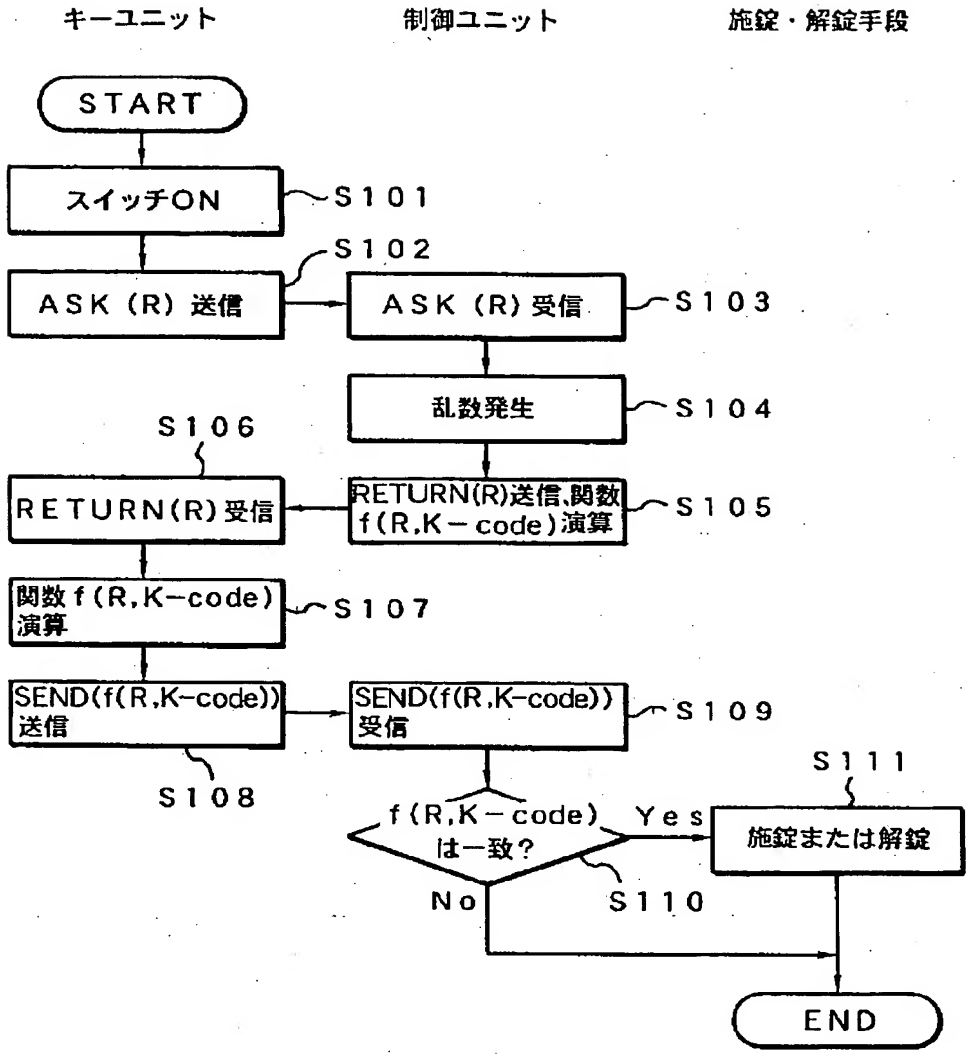
10、10a　キーユニット	12　情報送信手段
13　乱数受信手段	14a　第2の演算手段
15　第1の記憶手段	20、20a　制御ユニット
21　情報受信手段	22　乱数送信手段
23a　乱数発生手段	23b　第1の演算手段
23c　暗号判定手段	23d　動作指示手段
23e　暗証コード書き換え手段	24　第2の記憶手段
30　施錠・解錠手段	40　書き換え指示手段

【図1】



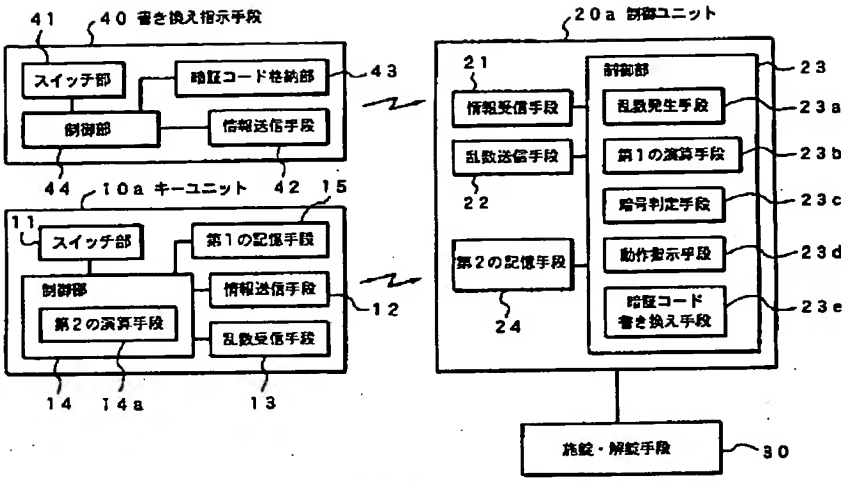
第1実施例の概略構成のブロック図

【図2】



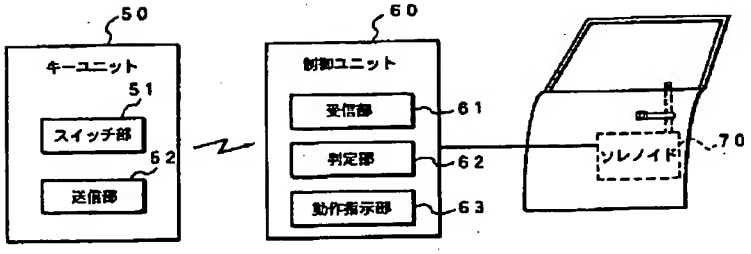
施錠／解錠の動作例のフローチャート

【図3】



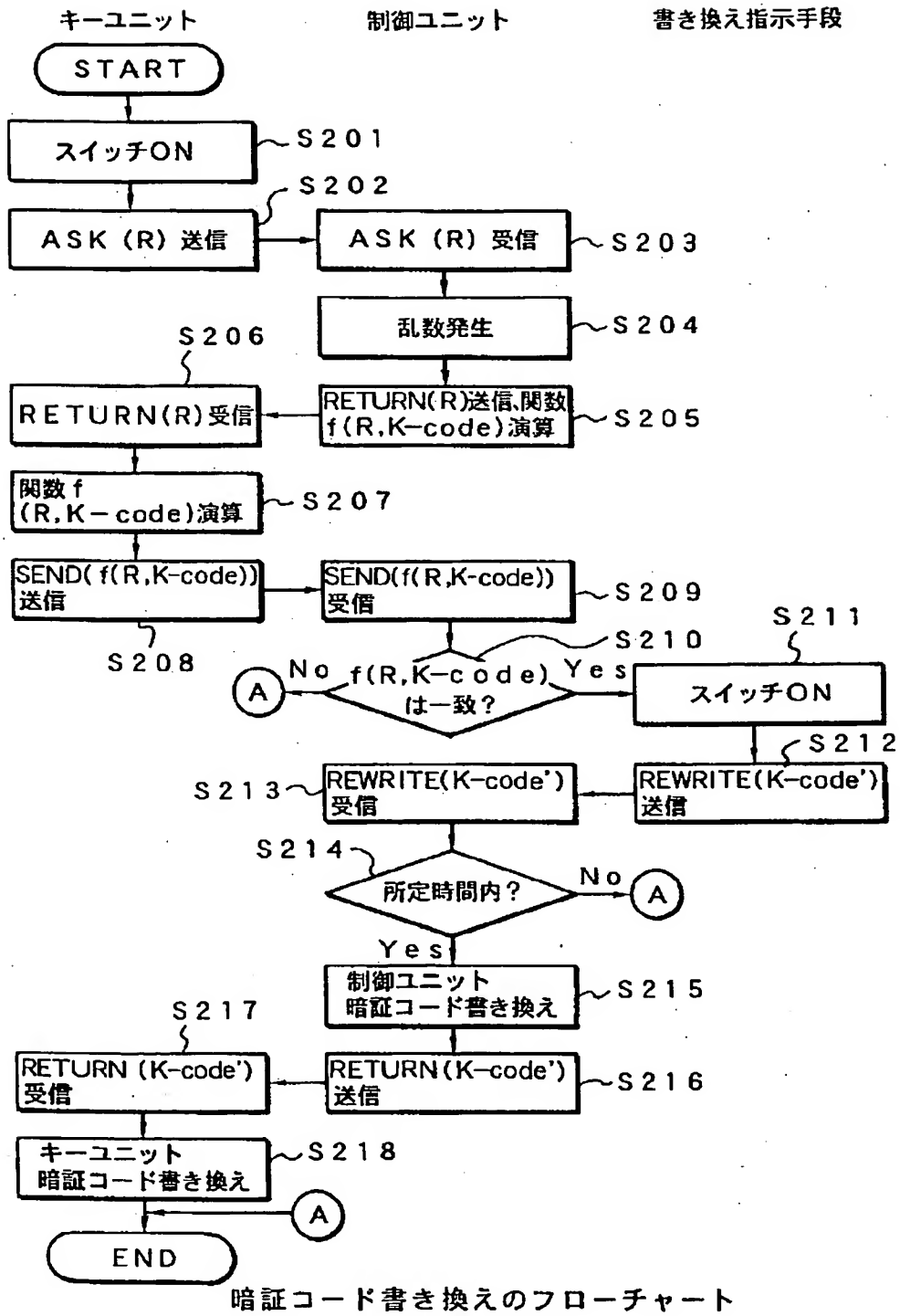
第2実施例の概略構成のブロック図

【図5】



従来例の概略構成のブロック図

【図4】



暗証コード書き換えのフローチャート